Kasami type codes of higher relative dimension

Chunlei Liu*†

Abstract

Let m, n, d, e be fixed positive integers such that

$$m = 2n,\ e = (n, d) = (m, d),\ 1 \leq k \leq \frac{n}{e}.$$

Let s be a fixed maximum-length binary sequence of length $2^m - 1$. For $0 \leq j < k$, let s_j be the circular decimation of s with decimation factor $2^{(\frac{n}{e}-j)d} + 1$. Then $s, s_1, \cdots, s_{k-1}$ are maximum-length binary sequences of length $2^m - 1$, while s_0 is a maximum-length binary sequence of length $2^n - 1$. Let C be the $\mathbb{F}_2$-vector space generated by all circular shifts of $s, s_0, s_1, \cdots, s_{k-1}$. Then C has an $\mathbb{F}_{2^n}$-vector space structure, and is of dimension $2k + 1$ over $\mathbb{F}_{2^n}$. We regard C as a Kasami type code of relative dimension $2k + 1$. The DC component distribution of C is explicitly calculated out in the present paper.

Key phrases: Kasami code, cyclic code, alternating form
MSC: 94B15, 11T71.

1 INTRODUCTION

Let q be a prime power, and C an $[n, k]$-linear code over $\mathbb{F}_q$. The weight of a codeword $c = (c_0, c_1, \cdots, c_{n-1})$ of C is defined to be

$$\mathrm{wt}(c) = \#\{0 \leq i \leq n-1 |\ c_i \neq 0\}.$$

For each $i = 0, 1, \cdots, n$, define

$$A_i = \#\{c \in C \mid\ \mathrm{wt}(c) = i\}.$$

The sequence $(A_0, A_1, \cdots, A_n)$ is called the weight distribution of C. Given a linear code C, it is challenging to determine its weight distribution. The weight distribution of Gold codes was determined by Gold [G66–G68]. The weight distribution of Kasami codes was determined by Kasami [K66]. The weight enumerators of Gold type and Kasami type codes of higher relative dimension were determined by Berlekamp [Ber] and Kasami [K71]. The weight distribution of some new Gold type codes of higher relative dimension was determined by Liu [Liu]. The weight distribution of the p-ary

*Dept. of math., Shanghai Jiao Tong Univ., Sahnghai 200240, China, clliu@sjtu.edu.cn.
†Dengbi Technologies Cooperation Limited, Yichun 336099, China, 714232747@qq.com.

analogue of Gold codes was determined by Trachtenberg [Tr]. The weight distribution of the circular decimation of the p-ary analogue of Gold codes with decimation factor 2 was determined by Feng-Luo [FL]. The weight distribution of the p-ary analogue of Gold type codes of relative dimension 3 was determined by Zhou-Ding-Luo-Zhang [ZDLZ]. The weight distribution of the circular decimation with decimation factor 2 of the p-ary analogue of Gold type codes of relative dimension 3 was determined by Zheng-Wang-Hu-Zeng [ZWHZ]. The weight distribution of the p-ary analogue of Kasami type codes of maximum dimension was determined by Li-Hu-Feng-Ge [LHFG]. The weight distribution of the p-ary analogue of Gold type codes of higher relative dimension was determined by Schmidt [Sch]. The weight distribution of some other classes of cyclic codes was determined in the papers [AL], [BEW], [BMC], [BMC10], [BMY], [De], [DLMZ], [DY], [FE], [FM], [KL], [LF], [LHFG], [LN], [LYL], [LTW], [MCE], [MCG], [MO], [MR], [MY], [MZLF], [RP], [SC], [VE], [WTQYX], [XI], [XI12], [YCD], [YXDL] and [ZHJYC].

Let m, n, d, e be fixed positive integers such that

$$m = 2n,\ e = (n, d) = (m, d),\ 1 \leq k \leq \frac{n}{e}.$$

Let s be a fixed maximum-length binary sequence of length $2^m - 1$. For $0 \leq j < k$, let s_j be the circular decimation of s with decimation factor $2^{(\frac{n}{e}-j)d}+1$. Then $s, s_1, \cdots, s_{k-1}$ are maximum-length binary sequences of length $2^m - 1$, while s_0 is a maximum-length binary sequence of length $2^n - 1$. Let C be the $\mathbb{F}_2$-vector space generated by all circular shifts of $s, s_0, s_1, \cdots, s_{k-1}$. For each $\vec{a} \in \mathbb{F}_{2^n} \times \mathbb{F}_{2^m}^k$, define a quadratic form on the $\mathbb{F}_{2^e}$-vector space $\mathbb{F}_{2^m}$ by the formula

$$Q_{\vec{a}}(x) = \mathrm{Tr}_{\mathbb{F}_{2^n}/\mathbb{F}_{2^e}}(a_0 x^{2^{\frac{nd}{e}}+1}) + \sum_{j=1}^{k-1} \mathrm{Tr}_{\mathbb{F}_{2^m}/\mathbb{F}_{2^e}}(a_j x^{2^{(\frac{n}{e}-j)d}+1}) + \mathrm{Tr}_{\mathbb{F}_{2^m}/\mathbb{F}_{2^e}}(a_k x).$$

Then

$$C = \{c_{\vec{a}} = (c_{\vec{a},0}, \cdots, c_{\vec{a},2^m-2}) \mid \ \vec{a} \in \mathbb{F}_{2^n} \times \mathbb{F}_{2^m}^k\},$$

where

$$c_{\vec{a},i} = \mathrm{Tr}_{\mathbb{F}_{2^e}/\mathbb{F}_2}(Q_{\vec{a}}(\pi^{-i})),$$

with π being a primitive element of $\mathbb{F}_{2^m}$. The correspondence $\vec{a} \mapsto c_{\vec{a}}$ defines an $\mathbb{F}_{2^n}$-vector space structure on C, and C is of dimension $2k+1$ over $\mathbb{F}_{2^n}$. When $k = 1$, C is the Kasami code. So we call C a Kasami type code of relative dimension $2k+1$. If $d = e = 1$, C is the code studied by Kasami [K71].

One can prove the following.

Theorem 1.1 *If $c \in C$ is nonzero, then*

$$\mathrm{DC}(c) \in \{-1, -1 + \pm 2^{\frac{m}{2}+je} \mid \ j = 0, 1, 2, \cdots, k-1\},$$

where

$$\mathrm{DC}(c) = \sum_{i=0}^{2^m-2} (-1)^{c_i}$$

is the DC component of $c = (c_0, c_1, \cdots, c_{2^m-2}) \in C$.

The present paper is concerned with the frequencies

$$\alpha_{r,\varepsilon} = \#\{0 \neq c \in C \mid \ \mathrm{DC}(c) = -1 + \varepsilon 2^{m-\frac{er}{2}}\}, \ r = 0, 2, 4, \cdots, \frac{m}{e}. \tag{1}$$

The main result of the present paper is the following.

Theorem 1.2 *For each* $j = 0, 1, \cdots, k-1$, *and for each* $\varepsilon = \pm 1$, *we have*

$$\alpha_{\frac{m}{e}-2j,\varepsilon} = \frac{1}{2}(2^{m-2ej} + \varepsilon 2^{\frac{m}{2}-ej}) \sum_{v=j}^{k-1} (-1)^{v-j} 4^{e\binom{v-j}{2}} \binom{v}{j}_{4^e} \binom{\frac{m}{2e}}{v}_{4^e} (2^{n(2k-1-2v)+ev} - 1),$$

where $\binom{j}{i}_q$ *is the Gaussian binomial coefficient.*

From the above theorem one can deduce the following.

Theorem 1.3 *We have*

$$\begin{aligned} &\#\{c \in C \mid \ \mathrm{DC}(c) = -1\} \\ &= 2^{n(2k+1)} - 1 - \sum_{v=0}^{k-1} (-1)^v (2^{n(2k-1-2v)+ev} - 1) 2^{m-ev(v+1)} \prod_{j=0}^{v-1} (2^m - 4^{ej}) \\ &\approx 2^{n(2k+1)} \sum_{v=1}^{k-1} (-1)^{v-1} 2^{-ev^2}. \end{aligned}$$

If $d = e = 1$, then the weight enumerator of C is determined by Kasami [K71]. However, some extra calculations are needed to explicitly write out the coefficients of the weight enumerator in [K71].

2 ENTERING BILINEAR FORMS

In this section we shall prove Theorem 1.1. Note that

$$1 + \mathrm{DC}(c_{\vec{a}}) = \sum_{x \in \mathbb{F}_{2^m}} (-1)^{\mathrm{Tr}_{\mathbb{F}_{2^e}/\mathbb{F}_2}(Q_{\vec{a}}(x))}. \tag{2}$$

It is well-known that

$$\sum_{x \in \mathbb{F}_{2^m}} (-1)^{\mathrm{Tr}_{\mathbb{F}_{2^e}/\mathbb{F}_2}(Q_{\vec{a}}(x))} = \begin{cases} 0, & 2 \nmid \mathrm{rk}(Q_{\vec{a}}), \\ \pm 2^{m-e\cdot\frac{\mathrm{rk}(Q_{\vec{a}})}{2})}, & 2 | \mathrm{rk}(Q_{\vec{a}}). \end{cases} \tag{3}$$

Let

$$B_{\vec{a}}(x,y) = Q_{\vec{a}}(x+y) - Q_{\vec{a}}(x) - Q_{\vec{a}}(y).$$

Then

$$B_{\vec{a}}(x,y) = \mathrm{Tr}_{\mathbb{F}_{2^n}/\mathbb{F}_{2^e}}(a_0(xy^{2^{\frac{nd}{e}}} + x^{2^{\frac{nd}{e}}}y)) + \sum_{j=1}^{k-1} \mathrm{Tr}_{\mathbb{F}_{2^m}/\mathbb{F}_{2^e}}(a_j(xy^{2^{(\frac{n}{e}-j)d}} + x^{2^{(\frac{n}{e}-j)d}}y)).$$

It is well-known that

$$\mathrm{rk}(B_{\vec{a}}) = \begin{cases} \mathrm{rk}(Q_{\vec{a}}), & 2 \mid \mathrm{rk}(Q_{\vec{a}}), \\ \mathrm{rk}(Q_{\vec{a}}) - 1, & 2 \nmid \mathrm{rk}(Q_{\vec{a}}). \end{cases} \tag{4}$$

We now prove Theorem 1.1. By (2), (3) and (4), it suffices to prove the following.

Theorem 2.1 *If* $(a_0, a_1, \cdots, a_{k-1}) \neq 0$*, then*

$$\mathrm{rk}(B_{\vec{a}}) \geq \frac{m}{e} - 2(k-1).$$

Proof. Suppose that $(a_0, a_1, \cdots, a_{k-1}) \neq 0$. It suffices to show that

$$\dim_{\mathbb{F}_{2^e}} \mathrm{Rad}(B_{\vec{a}}) \leq 2(k-1),$$

where

$$\mathrm{Rad}(B_{\vec{a}}) = \{x \in \mathbb{F}_{2^m} \mid \ B_{\vec{a}}(x,y) = 0, \ \forall y \in \mathbb{F}_{2^m}\}.$$

We have

$$\mathrm{Rad}(B_{\vec{a}}) = \{x \in \mathbb{F}_{2^m} \mid \ a_0 x^{2^{\frac{nd}{e}}} + \sum_{j=1}^{k-1}(a_j^{2^{(j-\frac{n}{e})d}} x^{2^{(j-\frac{n}{e})d}} + a_j x^{2^{(\frac{n}{e}-j)d}}) = 0\}$$

$$= \{x \in \mathbb{F}_{2^m} \mid \ a_0^{2^{(\frac{n}{e}+k-1)d}} x^{2^{k-1}} + \sum_{j=1}^{k-1}(a_j^{2^{(k-1+j)d}} x^{2^{(k-1+j)d}} + a_j^{2^{(\frac{n}{e}+k-1)d}} x^{2^{(k-1-j)d}}) = 0\}.$$

Note that

$$\{x \in \mathbb{F}_{2^{md/e}} \mid \ a_0^{2^{(\frac{n}{e}+k-1)d}} x^{2^{k-1}} + \sum_{j=1}^{k-1}(a_j^{2^{(k-1+j)d}} x^{2^{(k-1+j)d}} + a_j^{2^{(\frac{n}{e}+k-1)d}} x^{2^{(k-1-j)d}}) = 0\}.$$

is a subspace of $\mathbb{F}_{2^{md/e}}$ over $\mathbb{F}_{2^d}$ of dimension $\leq 2(k-1)$. As $(m,d) = e$, a basis of $\mathbb{F}_{2^m}$ over $\mathbb{F}_{2^e}$ is also a basis of $\mathbb{F}_{2^{md/e}}$ over $\mathbb{F}_{2^d}$. It follows that

$$\dim_{\mathbb{F}_{2^e}} \mathrm{Rad}(B_{\vec{a}}) \leq 2(k-1).$$

The theorem is proved. ■

3 AN INVERSION FORMULA

Let q be a prime power. In this section we shall prove an inversion formula for the symmetric van der Monte matrix $(q^{ij})_{0\le i,j\le u}$. We begin with the following well-known formula.

Theorem 3.1 (q-binomial Möbius inversion formula) *Suppose that $u > v$. Then the vector $(\binom{i}{v}_q)_{i=v}^u$ is orthogonal to the vector $((-1)^{u-i}q^{\binom{u-i}{2}}\binom{u}{i}_q)_{i=v}^u$, and the vector $(\binom{u}{i}_q)_{i=v}^u$ is orthogonal to the vector $((-1)^{i-v}q^{\binom{i-v}{2}}\binom{i}{v}_q)_{i=v}^u$.*

We now prove the following.

Theorem 3.2 (Inversion of a symmetric van der Monte matrix) *We have*

$$\sum_{j=0}^{u} q^{ij}x_j = y_i,\ 0 \le i \le u$$

if and only if

$$x_j = \sum_{v=j}^{u}(-1)^{v-j}q^{\binom{v-j}{2}}\binom{v}{j}_q \prod_{i=0}^{v-1}(q^v - q^i)^{-1}\sum_{i=0}^{v}(-1)^{v-i}q^{\binom{v-i}{2}}\binom{v}{i}_q y_i.$$

Proof. Fix $0 \le v \le u$. Consider the equation

$$\sum_{j=0}^{u} x_j \begin{pmatrix} 1 \\ q^j \\ \vdots \\ q^{vj} \end{pmatrix} = \begin{pmatrix} y_0 \\ y_1 \\ \vdots \\ y_v \end{pmatrix}$$

Multiplying on the left by the row vector $((-1)^{v-i}q^{\binom{v-i}{2}}\binom{v}{i}_q)_{i=0}^v$, and applying the q-binomial formula, we arrive at

$$\sum_{j=v}^{u} x_j \prod_{i=0}^{v-1}(q^j - q^i) = \sum_{i=0}^{v}(-1)^{v-i}q^{\binom{v-i}{2}}\binom{v}{i}_q y_i.$$

Dividing both sides by $\prod_{i=0}^{v-1}(q^v - q^i)$, we arrive at

$$\sum_{j=v}^{u} x_j \binom{j}{v}_q = \prod_{i=0}^{v-1}(q^v - q^i)^{-1}\sum_{i=0}^{v}(-1)^{v-i}q^{\binom{v-i}{2}}\binom{v}{i}_q y_i.$$

Applying q-binomial Möbius inversion formula, we arrive at

$$x_j = \sum_{v=j}^{u}(-1)^{v-j}q^{\binom{v-j}{2}}\binom{v}{j}_q \prod_{i=0}^{v-1}(q^v - q^i)^{-1}\sum_{i=0}^{v}(-1)^{v-i}q^{\binom{v-i}{2}}\binom{v}{i}_q y_i.$$

The theorem is proved.■

4 A PRODUCT FORMULA

Let q be a prime power. We begin with the following product formula.

Theorem 4.1 *If $i \geq 1$, then*

$$\sum_{j=0}^{i} q^j \binom{i}{j}_{q^2} = \prod_{j=1}^{i}(1+q^j).$$

Proof. The product formula in the theorem is trivial if $i = 1$. We now assume that $i \geq 2$. By the q-binomial recursion formula,

$$\begin{aligned}
&\sum_{j=0}^{i} q^j \binom{i}{j}_{q^2} \\
=&1+\sum_{j=1}^{i} q^j \left(\binom{i-1}{j}_{q^2} + \binom{i-1}{j-1}_{q^2} q^{2(i-j)}\right) \\
=&\sum_{j=0}^{i-1} q^j \binom{i-1}{j}_{q^2} + q^i \sum_{j=0}^{i-1} \binom{i-1}{j}_{q^2} q^{i-1-j} \\
=&(1+q^i)\sum_{j=0}^{i-1} q^j \binom{i-1}{j}_{q^2}.
\end{aligned}$$

The theorem now follows by induction. ■

We now prove the following product formula.

Theorem 4.2 *If $i \geq 1$, then*

$$\binom{u}{i}_{q^2} \sum_{j=0}^{i} q^j \binom{i}{j}_{q^2} = \binom{u}{i}_{q} \prod_{j=0}^{i-1}(1+q^{u-j}).$$

Proof. If $u = i$, the product formula in the theorem is precisely Theorem **??**. We now assume that $u \geq i+1$. We have

$$\begin{aligned}
\binom{u}{i}_{q^2} \prod_{j=0}^{i-1}(q^i+q^j) =& \binom{u}{i}_{q} \prod_{j=0}^{i-1}(q^u+q^j) \\
=& \binom{u}{i}_{q} \frac{q^u+1}{q^u+q^i} \prod_{j=1}^{i}(q^u+q^j) \\
=& \binom{u}{i}_{q} \frac{q^u+1}{q^{u-i}+1} \prod_{j=0}^{i-1}(q^{u-1}+q^j) \\
=& \binom{u}{i}_{q} \binom{u-1}{i}_{q^2} \binom{u-1}{i}_{q}^{-1} \frac{q^u+1}{q^{u-i}+1} \prod_{j=0}^{i-1}(q^i+q^j).
\end{aligned}$$

It follows that

$$\binom{u}{i}_{q^2} = \binom{u}{i}_{q} \binom{u-1}{i}_{q^2} \binom{u-1}{i}_{q}^{-1} \frac{q^u+1}{q^{u-i}+1}.$$

Hence, by induction,

$$\begin{aligned}
&\binom{u}{i}_{q^2}\sum_{j=0}^{i}q^j\binom{i}{j}_{q^2}\\
=&\binom{u}{i}_q\frac{q^u+1}{q^{u-i}+1}\binom{u-1}{i}_q^{-1}\binom{u-1}{i}_{q^2}\sum_{j=0}^{i}q^j\binom{i}{j}_{q^2}\\
=&\binom{u}{i}_q\frac{q^u+1}{q^{u-i}+1}\prod_{j=0}^{i-1}(1+q^{u-1-j})\\
=&\binom{u}{i}_q\prod_{j=0}^{i-1}(1+q^{u-j}).
\end{aligned}$$

The theorem is proved. ■

5 AN ELIMINATION METHOD

In this section we shall establish an elimination method for the system

$$\sum_{i=1}^{u}(x_{2i-1}x_{2i}^{2^{(\frac{n}{e}-j)d}}+x_{2i-1}^{2^{(\frac{n}{e}-j)d}}x_{2i})=0,\ j=0,1,2,\cdots,s. \tag{5}$$

Let $V_{s,u}$ be the set of solutions $(x_1,x_2,\cdots,x_{2u})\in\mathbb{F}_{2^m}^{2u}$ of the above system. We now prove the following.

Theorem 5.1 *The set $V_{s,u}$ is identical to the set of solutions $(x_1,x_2,\cdots,x_{2u})\in\mathbb{F}_{2^m}^{2u}$ of the system*

$$\begin{cases}\sum_{i=1}^{u}(x_{2i-1}x_{2i}^{2^{\frac{nd}{e}}}+x_{2i-1}^{2^{\frac{nd}{e}}}x_{2i})=0,\\ (\tilde{x}_1,\tilde{x}_2,\cdots,\tilde{x}_{2u})\in V_{s-1,u},\end{cases} \tag{6}$$

where $\tilde{x}_i=x_i+x_i^{2^{-d}}$.

Proof. In the system (5), adding 2^{-d}-th power of the $(j-1)$-th equation to the j-th equation, and adding $2^{\frac{nd}{e}}$-th power of the second equation to the first, we arrive at

$$\begin{cases}\sum_{i=1}^{u}(x_{2i-1}x_{2i}^{2^{\frac{nd}{e}}}+x_{2i-1}^{2^{\frac{nd}{e}}}x_{2i})=0,\\ \sum_{i=1}^{u}(x_{2i-1}x_{2i}^{2^{(\frac{n}{e}-j)d}}+x_{2i-1}^{2^{(\frac{n}{e}-j)d}}x_{2i}+x_{2i-1}^{2^{-d}}x_{2i}^{2^{(\frac{n}{e}-j)d}}+x_{2i-1}^{2^{(\frac{n}{e}-j)d}}x_{2i}^{2^{-d}})=0,\\ j=0,1,2,\cdots,s.\end{cases}$$

Adding the $(j-1)$-th equation to the j-th equation in the above system, we arrive at the system (6). The theorem is proved. ■

We now apply the above elimination method to prove the following.

Theorem 5.2 *If $s\geq u$ and $(x_1,x_2,\cdots,x_{2u})\in V_{s,u}$, then $x_1,x_2,x_4,x_6,\cdots,x_{2u}$ are linearly dependent over $\mathbb{F}_{2^e}$.*

Proof. The lemma is trivial if $u = 1$. Now assume that $u \geq 2$. We may assume that $x_{2u} \neq 0$. Then we may further assume that $x_{2u} = 1$. By Lemma 5.1, $(\tilde{x}_1, \tilde{x}_2, \cdots, \tilde{x}_{2u}) \in V_{s-1,u}$. As $\tilde{x}_{2u} = 0$, we see that $(\tilde{x}_1, \tilde{x}_2, \cdots, \tilde{x}_{2u-2}) \in V_{s-1,u-1}$. By induction, $(\tilde{x}_1, \tilde{x}_2, \tilde{x}_4, \tilde{x}_6, \cdots, \tilde{x}_{2u-2})$ are linearly dependent over $\mathbb{F}_{2^e}$. That is, there exists a nonzero vector $(\alpha_0, \alpha_1, \cdots, \alpha_{u-1}) \in \mathbb{F}_{2^e}^u$ such that $\alpha_0 \widetilde{x}_1 + \sum_{i=1}^{u-1} \alpha_i \widetilde{x}_{2i} = 0$. So,

$$\alpha_0 x_1 + \sum_{i=1}^{u-1} \alpha_i x_{2i} = (\alpha_0 x_1 + \sum_{i=1}^{u-1} \alpha_i x_{2i})^{2^{-d}}.$$

Set $\alpha_u = \alpha_0 x_1 + \sum_{i=1}^{u-1} \alpha_i x_{2i}$. Then $\alpha_u \in \mathbb{F}_{2^e}$, and $\alpha_0 x_1 + \sum_{i=1}^{u} \alpha_i x_{2i} = 0$. Therefore $x_1, x_2, x_4, \cdots, x_{2u}$ are linearly dependent over $\mathbb{F}_{2^e}$. The theorem is proved. ■

6 COUNTING THE NUMBER OF SOLUTIONS

In this section we shall count the set $V_{s,u}$. For each $\vec{x} = (x_1, x_2, \cdots, x_{2u}) \in V_{s,u}$, define

$$Z(\vec{x}) = \{(c_1, c_2, \cdots, c_u) \in \mathbb{F}_{2^e}^u \mid \sum_{i=1}^{u} c_i x_{2i} = 0\}.$$

For each $\mathbb{F}_{2^e}$-subspace H of $\mathbb{F}_{2^e}^u$, define

$$V_{s,u,H} = \{(x_1, x_2, \cdots, x_{2u}) \in V_{s,u} \mid Z(\vec{x}) = H\},$$

and

$$W_{s,u,H} = \{(x_1, x_2, \cdots, x_{2u}) \in V_{s,u} \mid Z(\vec{x}) \supseteq H\} = \cup_{L \supseteq H} V_{s,u,L}.$$

We can prove the following.

Lemma 6.1 *If H is a $\mathbb{F}_{2^e}$-subspace of $\mathbb{F}_{2^e}^u$ of dimension i, then*

$$|W_{s,u,H}| = 2^{mi} |V_{s,u-i}|.$$

Proof. Suppose that H is generated by the row vectors of a matrix A over $\mathbb{F}_{2^e}$. We may assume that $A \neq 0$. Changing the order of the variables if necessary, we may further the last column of A is $(1, 0, \cdots, 0)^{\mathrm{T}}$, where T denotes the transposition. That is , A is of the form

$$\begin{pmatrix} \alpha & 1 \\ B & 0 \end{pmatrix},$$

where $\alpha = (\alpha_1, \alpha_2, \cdots, \alpha_{u-1}) \in \mathbb{F}_{2^e}^{u-1}$. Then $W_{s,u,H}$ is the set of solutions $(x_1, \cdots, x_{2u})$ in $\mathbb{F}_{2^m}^{2u}$ of the system

$$\begin{cases} \sum_{i=1}^{u} (x_{2i-1} x_{2i}^{2^{(\frac{n}{e}-j)d}} + x_{2i-1}^{2^{(\frac{n}{e}-j)d}} x_{2i}) = 0, \ j = 1, 2, \cdots, s, \\ B(x_2, x_4, \cdots, x_{2u-2})^{\mathrm{T}} = 0 \\ x_{2u} = \alpha_1 x_2 + \alpha_2 x_4 + \cdots + \alpha_{u-1} x_{2u-2}. \end{cases}$$

Replacing $x_{2i-1}+\alpha_i x_{2u-1}$ with x_{2i-1}, $i=1,2,\cdots,u-1$, we conclude that the above system is equivalent to the system

$$\begin{cases}\sum_{i=1}^{u-1}(x_{2i-1}x_{2i}^{2^{(\frac{n}{e}-j)d}}+x_{2i-1}^{2^{(\frac{n}{e}-j)d}}x_{2i})=0,\ j=0,1,2,\cdots,s,\\ B(x_2,x_4,\cdots,x_{2u-2})^{\mathrm{T}}=0,\\ x_{2u}=\alpha_1x_2+\alpha_2x_4+\cdots+\alpha_{u-1}x_{2u-2},\\ x_{2u-1}\text{ free.}\end{cases}$$

The lemma now follows by induction. ■

We can also prove the following.

Lemma 6.2 *For $s\geq u\geq 2$, we have*

$$|V_{s,u,\{0\}}|=2^{eu(u+1)/2}\prod_{i=0}^{u-1}(2^m-2^{ei}).$$

Proof. It suffices to show that

$$|V_{s,u,\{0\}}|=2^{eu}(2^m-2^{e(u-1)})|V_{s,u-1,\{0\}}|.$$

By Theorem 5.2, it suffices to show that, for each $(\alpha_1,\alpha_2,\cdots,\alpha_u)\in\mathbb{F}_{2^e}^u$, the number of solutions $(x_1,x_2,\cdots,x_{2u})$ in $\mathbb{F}_{2^m}$ of the system

$$\begin{cases}\sum_{i=1}^{u}(x_{2i-1}x_{2i}^{2^{(\frac{n}{e}-j)d}}+x_{2i-1}^{2^{(\frac{n}{e}-j)d}}x_{2i})=0,\ j=0,1,\cdots,s,\\ x_1=\alpha_1x_2+\alpha_2x_4+\cdots+\alpha_ux_{2u},\\ x_2,x_4,\cdots,x_{2u}\text{ are linearly independent over }\mathbb{F}_{2^e}\end{cases}$$

is equal to $(2^m-2^{e(u-1)})V_{s,u-1,\{0\}}$. Replacing x_{2i-1} with $x_{2i-1}+\alpha_ix_2$ for each $i\geq 2$, we see that the above system is equivalent to the system

$$\begin{cases}\sum_{i=2}^{u}(x_{2i-1}x_{2i}^{2^{(\frac{n}{e}-j)d}}+x_{2i-1}^{2^{(\frac{n}{e}-j)d}}x_{2i})=0,\ j=0,1,\cdots,s,\\ x_1=\alpha_1x_2+\alpha_2x_4+\cdots+\alpha_ux_{2u},\\ x_2,x_4,\cdots,x_{2u}\text{ are linearly independent over }\mathbb{F}_{2^e},\end{cases}$$

whose number of solutions is precisely $(2^m-2^{e(u-1)})V_{s,u-1,\{0\}}$. The lemma now follows. ■

Applying the q-binomial Möbius inversion formula, we arrive at the following.

Corollary 6.3 *If $s\geq u\geq 1$, then*

$$\sum_{i=0}^{u}(-1)^{u-i}2^{e\binom{u-i}{2}}\binom{u}{i}_{2^e}2^{-mi}|V_{s,i}|=2^{eu(u+1)/2}\prod_{i=0}^{u-1}(1-2^{ei-m}),$$

where $|V_{s,0}|=1$.

Applying the q-binomial Möbius inversion formula once more, we arrive at the following.

Theorem 6.4 *If $s\geq i\geq 1$, then*

$$|V_{s,i}|=2^{mi}\sum_{u=0}^{i}\binom{i}{u}_{2^e}2^{eu(u+1)/2}\prod_{j=0}^{u-1}(1-2^{ej-m}).$$

7 A RECURSIVE RELATION

In this section we shall prove an useful recursive relation for $|V_{s,i}|$. We begin with the following.

Lemma 7.1 *If $s \geq i \geq 1$, then*

$$2^{-mi}|V_{s,i}| = \sum_{j=0}^{i}(-1)^j 4^{e\binom{j}{2}} 2^{-mj} \binom{i}{j}_{4^e} \sum_{u=0}^{i-j} 2^{eu} \binom{i-j}{u}_{4^e}.$$

Proof. By Theorem 6.4, and by the q-binomial formula, we have

$$2^{-mi}|V_{s,i}| = \sum_{u=0}^{i} \binom{i}{u}_{2^e} 2^{eu(u+1)/2} \sum_{j=0}^{u}(-1)^j 2^{e\binom{j}{2}} \binom{u}{j}_{2^e} 2^{-mj}.$$

Changing the order of summation, we arrive at

$$2^{-mi}|V_{s,i}| = \sum_{j=0}^{i}(-1)^j 2^{e\binom{j}{2}} 2^{-mj} \sum_{u=j}^{i} 2^{eu(u+1)/2} \binom{i}{u}_{2^e} \binom{u}{j}_{2^e}.$$

Applying the identity

$$\binom{i}{u}_{2^e} \binom{u}{j}_{2^e} = \binom{i}{j}_{2^e} \binom{i-j}{u-j}_{2^e},$$

we arrive at

$$2^{-mi}|V_{s,i}| = \sum_{j=0}^{i}(-1)^j 2^{2e\binom{j}{2}} 2^{-mj} \binom{i}{j}_{2^e} \sum_{u=0}^{i-j} 2^{e\binom{u}{2}} \binom{i-j}{u}_{2^e} 2^{euj}.$$

Applying the q-binomial formula, we arrive at

$$2^{-mi}|V_{s,i}| = \sum_{j=0}^{i}(-1)^j 2^{ej^2} 2^{-mj} \binom{i}{j}_{2^e} \prod_{u=0}^{i-j-1} (1 + 2^{e(i-u)}).$$

Applying Theorem 4.2, we arrive at

$$2^{-mi}|V_{s,i}| = \sum_{j=0}^{i}(-1)^j 2^{ej^2} 2^{-mj} \binom{i}{j}_{4^e} \sum_{u=0}^{i-j} 2^{eu} \binom{i-j}{u}_{4^e}.$$

The lemma is proved. ■

We now prove the following.

Theorem 7.2 *If $s \geq i \geq 1$, then*

$$\sum_{i=0}^{v}(-1)^{v-i} 4^{e\binom{v-i}{2}} \binom{v}{i}_{4^e} 2^{-mi}|V_{s,i}| = 2^{(e-m)v} \prod_{j=0}^{v-1}(2^m - 4^{ej}).$$

Proof. By Lemma 7.1, we have

$$\begin{aligned}
&\sum_{i=0}^{v}(-1)^{v-i}4^{e\binom{v-i}{2}}\binom{v}{i}_{4^e}2^{-mi}|V_{s,i}| \\
=&\sum_{i=0}^{v}(-1)^{v-i}4^{e\binom{v-i}{2}}\binom{v}{i}_{4^e}\sum_{j=0}^{i}(-1)^j2^{ej^2}2^{-mj}\binom{i}{j}_{4^e}\sum_{u=0}^{i-j}2^{eu}\binom{i-j}{u}_{4^e} \\
=&\sum_{j=0}^{v}(-1)^j2^{ej^2}2^{-mj}\sum_{i=j}^{v}(-1)^{v-i}4^{e\binom{v-i}{2}}\binom{v}{i}_{4^e}\binom{i}{j}_{4^e}\sum_{u=0}^{i-j}2^{eu}\binom{i-j}{u}_{4^e} \\
=&\sum_{j=0}^{v}(-1)^j2^{ej^2}2^{-mj}\sum_{u=0}^{v-j}2^{eu}\sum_{i=u+j}^{v}(-1)^{v-i}4^{e\binom{v-i}{2}}\binom{v}{i}_{4^e}\binom{i}{j}_{4^e}\binom{i-j}{u}_{4^e}.
\end{aligned}$$

Applying the identity

$$\binom{v}{u}_{4^e}\binom{v-u}{i-u}_{4^e}\binom{i-u}{j}_{4^e}=\binom{v}{i}_{4^e}\binom{i}{j}_{4^e}\binom{i-j}{u}_{4^e},$$

we arrive at

$$\begin{aligned}
&\sum_{i=0}^{v}(-1)^{v-i}4^{e\binom{v-i}{2}}\binom{v}{i}_{4^e}2^{-mi}|V_{s,i}| \\
=&\sum_{j=0}^{v}(-1)^j2^{ej^2}2^{-mj}\sum_{u=0}^{v-j}2^{eu}\binom{v}{u}_{4^e}\sum_{i=j}^{v-u}(-1)^{v-i-u}4^{e\binom{v-i-u}{2}}\binom{v-u}{i}_{4^e}\binom{i}{j}_{4^e}.
\end{aligned}$$

Applying the q-binomial Möbius inversion formula, we arrive at

$$\sum_{i=0}^{v}(-1)^{v-i}4^{e\binom{v-i}{2}}\binom{v}{i}_{4^e}2^{-mi}|V_{s,i}|=2^{ev}\sum_{j=0}^{v}(-1)^j4^{e\binom{j}{2}}\binom{v}{j}_{4^e}2^{-mj}.$$

Applying the q-binomial formula, we arrive at

$$\sum_{i=0}^{v}(-1)^{v-i}4^{e\binom{v-i}{2}}\binom{v}{i}_{4^e}2^{-mi}|V_{s,i}|=2^{(e-m)v}\prod_{j=0}^{v-1}(2^m-4^{ej}).$$

■

8 ENTERING BILINEAR EQUATIONS

In this section we shall prove Theorem 1.2. We begin with the following.

Theorem 8.1 *For each $r=0,2,\cdots,\frac{m}{e}$,*

$$\alpha_{r,\varepsilon}=\frac{1}{2}(2^{er}+\varepsilon 2^{\frac{er}{2}})\beta_r,$$

where

$$\beta_r=2^{-m}\#\{\vec{a}\in\mathbb{F}_{2^n}\times\mathbb{F}_{2^m}^k\mid \operatorname{rk}(B_{\vec{a}})=r,\ (a_0,a_1,\cdots,a_{k-1})\neq 0\}. \qquad (7)$$

Proof. By (1), (2), (3), (4), and (7),

$$
\begin{aligned}
&2^{m-\frac{er}{2}}(\alpha_{r,1}-\alpha_{r,-1})\\
&=\sum_{\mathrm{rk}(B_{\vec{a}})=r}\sum_{x\in\mathbb{F}_{2^m}}(-1)^{\mathrm{Tr}_{\mathbb{F}_{2^e}/\mathbb{F}_2}(Q_{\vec{a}}(x))}\\
&=2^{-m}\sum_{c\in\mathbb{F}_{2^m}}\sum_{\mathrm{rk}(B_{\vec{a}})=r}\sum_{x\in\mathbb{F}_{2^m}}(-1)^{\mathrm{Tr}_{\mathbb{F}_{2^e}/\mathbb{F}_2}(\mathrm{Tr}_{\mathbb{F}_{2^m}/\mathbb{F}_{2^e}}(cx)+Q_{\vec{a}}(x))}\\
&=2^{-m}\sum_{\mathrm{rk}(B_{\vec{a}})=r}\sum_{x\in\mathbb{F}_{2^m}}(-1)^{\mathrm{Tr}_{\mathbb{F}_{2^e}/\mathbb{F}_2}(Q_{\vec{a}}(x))}\sum_{c\in\mathbb{F}_{2^m}}(-1)^{\mathrm{Tr}_{\mathbb{F}_{2^m}/\mathbb{F}_2}(cx)}\\
&=2^m\beta_r.
\end{aligned}
$$

Similarly,

$$
\begin{aligned}
&2^{2m-er}(\alpha_{r,1}+\alpha_{r,-1})\\
&=\sum_{\mathrm{rk}(B_{\vec{a}})=r}\Big(\sum_{x\in\mathbb{F}_{2^m}}(-1)^{\mathrm{Tr}_{\mathbb{F}_{2^e}/\mathbb{F}_2}(Q_{\vec{a}}(x))}\Big)^2\\
&=2^{-m}\sum_{c\in\mathbb{F}_{2^m}}\sum_{\mathrm{rk}(B_{\vec{a}})=r}\Big(\sum_{x\in\mathbb{F}_{2^m}}(-1)^{\mathrm{Tr}_{\mathbb{F}_{2^e}/\mathbb{F}_2}(\mathrm{Tr}_{\mathbb{F}_{2^m}/\mathbb{F}_{2^e}}(cx)+Q_{\vec{a}}(x))}\Big)^2\\
&=2^{-m}\sum_{\mathrm{rk}(B_{\vec{a}})=r}\sum_{x,y\in\mathbb{F}_{2^m}}(-1)^{\mathrm{Tr}_{\mathbb{F}_{2^e}/\mathbb{F}_2}(Q_{\vec{a}}(x)+Q_{\vec{a}}(y))}\sum_{c\in\mathbb{F}_{2^m}}(-1)^{\mathrm{Tr}_{\mathbb{F}_{2^m}/\mathbb{F}_2}(c(x+y))}\\
&=2^{2m}\beta_r.
\end{aligned}
$$

The theorem is proved.■

By Theorem 8.1, Theorem 1.2 follows from the following.

Theorem 8.2 *For each $j=0,1,\cdots,k-1$, we have*

$$\beta_{\frac{m}{e}-2j,\varepsilon}=\sum_{v=j}^{k-1}(-1)^{v-j}4^{e\binom{v-j}{2}}\binom{v}{j}_{4^e}\binom{\frac{m}{2e}}{v}_{4^e}(2^{n(2k-1-2v)+ev}-1).$$

Proof. By the orthogonality of characters, we have

$$\sum_{\vec{a}\in\mathbb{F}_{2^n}\times\mathbb{F}_{2^m}^k}\Big(\sum_{x,y\in\mathbb{F}_{2^m}}(-1)^{\mathrm{Tr}_{\mathbb{F}_{2^e}/\mathbb{F}_2}(B_{\vec{a}}(x,y))}\Big)^u=2^{n(2k+1)}|V_{k-1,u}|,\ 0\le u\le k-1.$$

Applying the identity

$$\sum_{x,y\in\mathbb{F}_{2^m}}(-1)^{\mathrm{Tr}_{\mathbb{F}_{2^e}/\mathbb{F}_2}(B_{\vec{a}}(x,y))}=2^{2m-e\cdot\mathrm{rk}(B_{\vec{a}})},$$

we arrive at

$$\sum_{2|r=0}^{m/e}\beta_r2^{u(2m-er)}=2^{n(2k-1)}|V_{k-1,u}|-2^{2mu},\ 0\le u\le k-1.$$

Applying Theorem 2.1, we arrive at

$$\sum_{2|r=m/e-2(k-1)}^{m/e}\beta_r2^{u(2m-er)}=2^{n(2k-1)}|V_{k-1,u}|-2^{2mu},\ 0\le u\le k-1.$$

That is,

$$\sum_{i=0}^{k-1}\beta_{\frac{m}{e}-2i}4^{eiu}=2^{n(2k-1-2u)}|V_{k-1,u}|-2^{mu},\ 0\le u\le k-1.$$

Applying the inversion formula of a symmetric van der Monte matrix, we arrive at

$$\beta_{\frac{m}{e}-2j}=\sum_{v=j}^{k-1}(-1)^{v-j}4^{e\binom{v-j}{2}}\binom{v}{j}_{4^e}\prod_{i=0}^{v-1}(4^{ev}-4^{ei})^{-1}\sum_{i=0}^{v}(-1)^{v-i}4^{e\binom{v-i}{2}}\binom{v}{i}_{4^e}y_i,$$

where

$$y_i=2^{n(2k-1-2i)}|V_{k-1,i}|-2^{im}.$$

The contribution of -2^{im} to $\beta_{\frac{m}{e}-2j}$ is

$$\begin{aligned}&-\sum_{v=j}^{k-1}(-1)^{v-j}4^{e\binom{v-j}{2}}\binom{v}{j}_{4^e}\prod_{i=0}^{v-1}(4^{ev}-4^{ei})^{-1}\sum_{i=0}^{v}(-1)^{v-i}4^{e\binom{v-i}{2}}\binom{v}{i}_{4^e}2^{im}\\
=&-\sum_{v=j}^{k-1}(-1)^{v-j}4^{e\binom{v-j}{2}}\binom{v}{j}_{4^e}\prod_{i=0}^{v-1}(2^m-4^{ei})(4^{ev}-4^{ei})^{-1}\\
=&-\sum_{v=j}^{k-1}(-1)^{v-j}4^{e\binom{v-j}{2}}\binom{v}{j}_{4^e}\binom{\frac{m}{2e}}{v}_{4^e}.\end{aligned}$$

By Theorem 7.2, the contribution of $2^{n(2k-1-2i)}|V_{k-1,i}|$ to $\beta_{\frac{m}{e}-2j}$ is equal to

$$2^{n(2k-1)}\sum_{v=j}^{k-1}(-1)^{v-j}4^{e\binom{v-j}{2}}\binom{v}{j}_{4^e}2^{(e-m)v}.$$

∎

We now prove Theorem 1.3. We have

$$\begin{aligned}&\#\{c\in C\mid\ \mathrm{DC}(c)=-1\}\\
=&2^{n(2k+1)}-1-\sum_{j=0}^{k-1}2^{m-2ej}\sum_{v=j}^{k-1}(-1)^{v-j}4^{e\binom{v-j}{2}}\binom{v}{j}_{4^e}\binom{\frac{m}{2e}}{v}_{4^e}(2^{n(2k-1-2v)+ev}-1)\\
=&2^{n(2k+1)}-1-\sum_{v=0}^{k-1}\binom{\frac{m}{2e}}{v}_{4^e}(2^{n(2k-1-2v)+ev}-1)\sum_{j=0}^{v}2^{m-2ej}(-1)^{v-j}4^{e\binom{v-j}{2}}\binom{v}{j}_{4^e}\\
=&2^{n(2k+1)}-1-\sum_{v=0}^{k-1}(-1)^v\binom{\frac{m}{2e}}{v}_{4^e}(2^{n(2k-1-2v)+ev}-1)2^{m-2ev}\prod_{j=1}^{v}(4^{ej}-1)\\
=&2^{n(2k+1)}-1-\sum_{v=0}^{k-1}(-1)^v(2^{n(2k-1-2v)+ev}-1)2^{m-ev(v+1)}\prod_{j=0}^{v-1}(2^m-4^{ej})\\
\approx&2^{n(2k+1)}\sum_{v=1}^{k-1}(-1)^{v-1}2^{-ev^2}.\end{aligned}$$

Theorem 1.3 is proved.

Acknowledgement. The author thanks Kai-Uwe Schmidt for telling him some background of this subject.

References

[AL] Y. Aubry, P. Langevin, On the weights of binary irreducible cyclic codes, in Proc. Int. Conf. Cod. Cryptography, 2006, pp. 46-54.

[BMC] L. D. Baumert, R. J. McEliece, Weights of irreducible cyclic codes, Inf. Control, vol. 20, no. 2, pp. 158-175, 1972.

[BMY] L. D. Baumert, J. Mykkeltveit, Weight distributions of some irreducible cyclic codes, DSN Progress Rep., vol. 16, pp. 128-131, 1973.

[Ber] E. R. Berlekamp, The weight enumerators for certain subcodes of the 2nd order Reed-Muller codes, Inf. Contr., 17: 485-500, 1970.

[BEW] B. C. Berndt, R. J. Evans, K. S. Williams, Gauss and Jacobi Sums. New York, NY, USA: Wiley, 1997.

[BMC10] N. Boston, G. McGuire, The weight distributions of cyclic codes with two zeros and zeta functions, J. Symbol. Comput., vol. 45, no. 7, pp. 723-733, 2010.

[De] P. Delsarte, On subfield subcodes of modified reed-solomon codes, IEEE Trans. Inf. Theory, vol. 21, no. 5, pp. 575-576, 1975.

[DG] P. Delsarte, J.-M. Goethals, Alternating blinear forms over GF(q), J. Comb. Theory (A) 19 (1): 26-50, 1975.

[DLMZ] C. Ding, Y. Liu, C. Ma, L. Zeng, The weight distributions of the duals of cyclic codes with two zeros, IEEE Trans. Inf. Theory, vol. 57, no. 12, pp. 8000-8006, 2011.

[DY] C. Ding, J. Yang, Hamming weights in irreducible cyclic codes, Discr. Math., vol. 313, pp. 434-446, 2013.

[FL] K. Feng, J. Luo, Weight distribution of some reducible cyclic codes,Finite Fields Appl., vol. 14, no. 2, pp. 390-409, 2008.

[FE] T. Feng, On cyclic codes of length 2^{2^r} with two zeros whose dual codes have three weights, Des. Codes Cryptogr., vol. 62, pp. 253-258, 2012.

[FM] T. Feng K. Momihara, Evaluation of the weight distribution of a class of cyclic codes based on Index 2 Gauss sums, 2012, preprint.

[G66] R. Gold, Characteristic linear sequences and their coset functions, J. SIAM Appl. Math. 14 (5): 980-985, 1966.

[G67] R. Gold, Optimal binary sequences for spread spectrum multiplexing, IEEE Trans. Inform. Theory 13 (4): 619-621, 1967.

[G68] R. Gold, Maximal recursive sequences with 3-valued recursive cross-correlation functions, IEEE Trans. Inform. Theory 14 (1): 154-156, 1968.

[K66] T. Kasami, Weight distribution formula for some cyclic codes, Univ. of Illinois, Rept. R-265, 1966.

[K71] T. Kasami, Weight enumerators for several classes of subcodes of the 2nd order Reed-Muller codes, Inf. Contr., 18: 369-394, 1971.

[KL] T. Kløve, Codes for Error Detection. Hackensack, NJ, USA: World Scientific, 2007.

[LHFG] S. X. Li, S. H. Hu, T. Feng and G. Ge, The weight distribution of a class of cyclic codes related to Hermitian graphs, IEEE Trans. Inf. Theory, vol. 59, no. 5, pp. 3064-3067, 2013.

[LN] R. Lidl H. Nuederreuter, Finite Fields. NewYork, NY, USA: Addision-Wesley, 1983.

[Liu] C. Liu, Gold type code of higher relative dimension, arXiv:1506.01498.

[LYL] Y. Liu, H. Yan and C. Liu, A class of six-weight cyclic codes and their weight distribution, Des. Codes Cryptogr., to appear.

[LF] J. Luo K. Feng, On the weight distribution of two classes of cyclic codes, IEEE Trans. Inf. Theory, vol. 54, no. 12, pp. 5332-5344, Dec. 2008.

[LTW] J. Luo, Y. Tang, H. Wang, Cyclic codes and sequences: the generalized Kasami case, IEEE Trans. Inf. Theory, vol. 56, no. 5, pp. 2130-2142, May 2010.

[MZLF] C. Ma, L. Zeng, Y. Liu, D. Feng, C. Ding, The weight enumerator of a class of cyclic codes, IEEE Trans. Inf. Theory, vol. 57, no. 1, pp. 397-402, Jan. 2011.

[MCE] R. J. McEliece, Irreducible cyclic codes and Gauss sums, in Part 1: Theory of Designs, Finite Geometry and Coding Theory, Math. Centre Tracts, Math. Centrum, ser. Combinatorics: NATO Advanced Study Institute Series. Amsterdam, The Netherlands: Springer, 1974, pp. 179-196.

[MCG] G. McGuire, On three weights in cyclic codes with two zeros, Finite Fields Appl., vol. 10, no. 1, pp. 97-104, 2004.

[MO] M. Moisio, The moments of a Kloosterman sum and the weight distribution of a Zetterberg-type binary cyclic code, IEEE Trans. Inf. Theory, vol. 53, no. 2, pp. 843-847, Feb. 2007.

[MR] M. Moisio, K. Ranto, Kloosterman sum identities and low-weight codewords in a cyclic code with two zeros, Finite Fields Appl., vol. 13, no. 4, pp. 922-935, 2007.

[MY] G. Myerson, Period polynomials and Gauss sums for finite fields, Acta Arith., vol. 39, pp. 251-264, 1981.

[RP] A. Rao, N. Pinnawala, A family of two-weight irreducible cyclic codes, IEEE Trans. Inf. Theory, vol. 56, no. 6, pp. 2568-2570, Jun. 2010.

[SC] R. Schoof, Families of curves and weight distribution of codes, Bull. Amer. Math. Soc., vol. 32, no. 2, pp. 171C183, 1995.

[Sch] K. Schmidt, Symmetric bilinear forms over finite fields with applications to coding theory0, arXiv: 1410.7184.

[Tr] H. M. Trachtenberg, On the correlation functions of maximal linear recurring sequences, Ph. D. dissertation, Univ. Southern California, Los Angles, CA, USA, 1970.

[VE] G. Vega, The weight distribution of an extended class of reducible cyclic codes, IEEE Trans. Inf. Theory, vol. 58, no. 7, pp. 4862-4869, Jul. 2012.

[WTQYX] B. Wang, C. Tang, Y. Qi, Y. Yang, M. Xu, The weight distributions of cyclic codes and elliptic curves, IEEE Trans. Inf. Theory, vol. 58, no. 12, pp. 7253-7259, Dec. 2012.

[XI12] M. Xiong, The weight distributions of a class of cyclic codes, Finite Fields Appl., vol. 18, no. 5, pp. 933-945, 2012.

[XI] M. Xiong, The weight distributions of a class of cyclic codes II, Design Codes Cryptography, to be published.

[YXDL] J. Yang, M. Xiong, C. Ding and J. Luo, Weight distribution of a class of cyclic codes with arbitrary number of zeros, IEEE Trans. Inform. Theory, vol. 59, no. 9, pp. 5985-5993, 2013.

[YCD] J. Yuan, C. Carlet, C. Ding, The weight distribution of a class of linear codes from perfect nonlinear functions, IEEE Trans. Inf. Theory, vol. 52, no. 2, pp. 712-717, Feb. 2006.

[ZHJYC] X. Zeng, L. Hu, W. Jiang, Q. Yue, X. Cao, The weight distribution of a class of p-ary cyclic codes, Finite Fields Appl., vol. 16, no. 1, pp. 56-73, 2010.

[ZWHZ] D. Zheng, X. Wang, L. Hu, X. Zeng, The weight distribution of a class of p-ary cyclic codes, Finite Fields Appl. 16 (5): 933-945, 2012.

[ZDLZ] Z. Zhou, C. Ding, J. Luo, A. Zhang, A family of five-weight cyclic codes and their weight enumerators, IEEE Trans. Inf. Theory 59 (10): 6674-6682, 2013.